PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-006880
(43)Date of publication of application : 10.01.1997

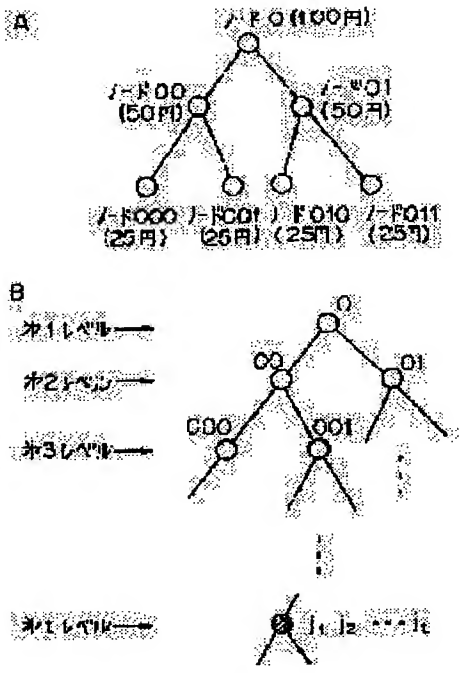
(51)Int.Cl. G06F 19/00
G06F 15/00
G07F 7/12
// G07B 1/00

(21)Application number : 08-203359
(22)Date of filing : 01.08.1996

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : OKAMOTO TATSUAKI
OTA KAZUO

(54) METHOD FOR DIVISIONAL USE OF ELECTRONIC CASH

(57)Abstract:
PROBLEM TO BE SOLVED: To enable the divisional use of electronic cash.
SOLUTION: A hierarchical structure table which has the face value (e.g. 100 yen) of the electronic cash set at the top and a use minimum unit (e.g. 75 yen) at the bottom is generated, and a rule wherein (1) the total of the corresponding amounts of child nodes right below one node is equal to the amount of the node and (2) when one node is used once, all the ancestor nodes and descendant nodes connected to the node are not used is applied. For example, when 75 yen is used, nodes 00 and 010 are used.



LEGAL STATUS

[Date of request for examination]	01.08.1996
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2879792
[Date of registration]	29.01.1999
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－6880

(43)公開日　平成９年(1997)１月10日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	19/00			Ｇ０６Ｆ	15/30	３４０
	15/00	３９０	9364－5L		15/00	３９０
Ｇ０７Ｆ	7/12			Ｇ０７Ｂ	1/00	Ｅ
// Ｇ０７Ｂ	1/00			Ｇ０６Ｆ	15/30	Ｚ
						３６０

審査請求　有　　請求項の数３　ＯＬ　（全 12 頁）　最終頁に続く

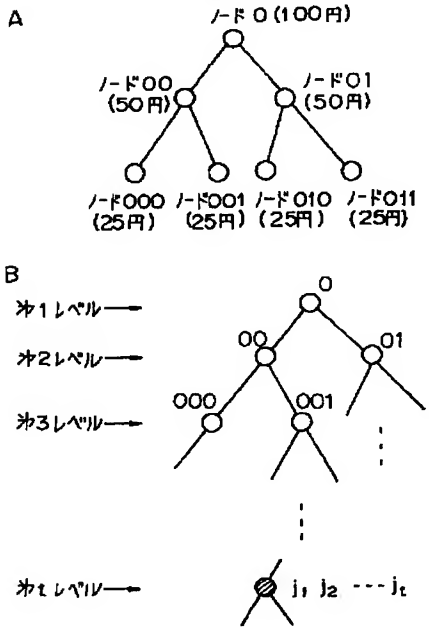
(21)出願番号　特願平8－203359
(62)分割の表示　特願平3－143530の分割
(22)出願日　平成３年(1991)６月14日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(72)発明者　岡本　龍明
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(72)発明者　太田　和夫
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(74)代理人　弁理士　草野　卓

(54)【発明の名称】　電子現金の分割使用方法

(57)【要約】
【課題】　電子現金の分割使用を可能とする。
【解決手段】　電子現金の額面（例えば１００円）を階層的構造テーブルの最上位とし、使用最小単位（例えば７５円）を階層的構造テーブルの最下位層としたテーブルを定め、（１）このテーブルにはあるノードの直下の子ノードの該当金額の合計が、そのノードの該当金額となる、（２）あるノードが一度使われた後は、そのノードと連結するすべての先祖ノードにおよび子孫ノードは利用しないというルールを適用する。例えば７５円を使う場合は、ノード００とノード０１０を用いる。

図７



1

【特許請求の範囲】

【請求項１】　電子現金の額面を階層的構造テーブルの最上位ノードとし、使用最小単位を階層的構造テーブルの最下位層のノードとし、あるノードの直下の子ノードの該当金額の合計が、そのノードの該当金額とする階層的構造テーブルを定め、

使用金額をノードで指定し、

あるノードが一度使われた後は、そのノードのすべての先祖ノード、およびすべての子孫ノードは利用しない、かつ各ノードは１回以上使用しないというルールを適用する電子現金の分割使用方法。

【請求項２】　電子現金を利用する者（以下、利用者という）が有する装置（以下、利用者側装置という）と、利用者より電子現金を受領する機関（以下、小売店という）が有する装置（以下、小売店側装置という）により電子現金を分割使用する請求項１記載の方法において、

上記利用者側装置は電子現金の額面と対応した値Γ。を生成し、上記階層構造における使用金額と対応したノードと対応した値$\Omega_{i_1,\ldots,i_1}$を生成し、

上記値Γ。と上記値$\Omega_{i_1,\ldots,i_1}$（Ｌ＝１，…，ｔ）を用いて、上記使用金額に対応するノードに対する値の剰余べき乗根

【数１】

$$X_{j_1\cdots j_t}=\left[\left(\Omega_{j_1\cdots j_t}^{2^{t-1}j_t}\Omega_{j_1\cdots j_{t-1}}^{2^{t-2}j_{t-1}}\cdots\Omega_{j_1}^{2j_2}\Gamma_0\right)^{1/2^t}\bmod N\right]_{-1}$$

を求め、〔…〕$_{-1}$はヤコビ記号であって、（$x_{i_1\ldots i_t}$／Ｎ）＝－１であり、

この$x_{i_1\ldots i_t}$および電子現金を上記小売店側装置へ送り、

上記小売店側装置は上記受信した$x_{i_1\ldots i_t}$が（$x_{i_1i_1\ldots i_t}$／Ｎ）＝－１を満たすかを検証し、

利用者側装置と同様の処理によりΓ。と$\Omega_{i_1i_1\ldots i_1}$を生成し、

【数２】

$$X_{j_1\cdots j_t}^{2^t}=d\,\Omega_{j_1\cdots j_{t-1}}^{2^{t-1}j_t}\Omega_{j_1\cdots j_{t-2}}^{2^{t-2}j_{t-2}}\cdots\Omega_{j_1}^{2j_2}\Gamma_0\bmod N$$

を満たすかを検証し、

以上の検証が正しければ、上記電子現金による上記使用金額の支払いを認める。

【請求項３】　電子現金を利用するる者（以下、利用者という）が有する装置（以下、利用者側装置という）と、

利用者より電子現金を受信する機関（以下、小売店という）が有する装置（以下、小売店側装置という）により電子現金を分割使用する請求項１または２記載の方法において、

小売店側装置は値Ｅ（＝０または１）を利用者側装置へ送り、

2

利用者側装置は電子現金の額面および使用金額ノードと対応した値$\Lambda_{i_1\ldots i_t}$を生成し、

値$\Lambda_{i_1\ldots i_t}$と値Ｅとから次の剰余平方根演算を行い、

$Y_{i_1\ldots i_t}=\{(\Lambda_{i_1\ldots i_t})^{Y_2}\bmod N\}_{(-1)^E}$

この$Y_{i_1\ldots i_t}$を小売店側装置へ送り、

小売店側装置は受信した$Y_{i_1\ldots i_t}$について

$(Y_{i_1\ldots i_t}/N)=(-1)^E$

$(Y_{i_1\ldots i_t})^2=d'\,f\Lambda(C\|_{i_1}\|\cdots\|_{i_t}\|N)\bmod N$

を共に満足するかを検証し、正しければ上記電子現金による上記使用金額の支払いを認める。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、電気通信システムやＩＣカードなどを用いて電子現金による支払い、譲渡などを行う際に、電子現金をその額面の範囲内で分割使用する電子現金の分割使用方法に関する。

【０００２】

【従来の技術】電気通信システムを用いた電子資金移動が普及しつつある。一般に換金可能な証書（手形、小切手など）は、証書の象徴的機能（証書を保持している人に対して、証書に記載してある権利が供与されること）を備えている。証書を電気通信システムで取り扱う場合、証書はディジタル化されたデータであり、容易にコピーを作成して複数回の換金が可能となる。プリペイドカードのような電子的現金を実現するときにも、この問題が生じる。すなわち、プリペイドカードをコピーすることで、不正に複数回の換金あるいは商品の購入が可能となる。一方、クレジットカードでは、このような２重使用の危険性はほとんどないが、その代わりに、利用者の利用履歴がすべてカード会社に知られてしまうという欠点がある（つまり、プライバシが保証されていない）。これら問題の解決策として、計算機能を備えたカードで換金時にカード読み取り装置とカードとの間のデータのやりとりを工夫することで、プライバシを保証し、かつカードの２重使用を検出する方式が提案されている。たとえば、Ｃｈａｕｍ，Ｆｉａｔ，Ｎａｏｒ：“Ｕｎｔｒａｃｅａｂｌｅ　Ｅｌｅｃｔｒｉｃ　Ｃａｓｈ”，Ｐｒｏｃ．ｏｆ　ＣＲＹＰＴＯ’８８がある。しかしながら、Ｃｈａｕｍ等の方式では、一回発行された電子現金を分割して利用する（例えば、１万円の電子現金を合計利用額が１万円になるまで何回も利用する）ことはできない。また、Ｃｈａｕｍ等の方式では、一回毎の電子現金発行時に、銀行と利用者の間でかなりの量の通信と処理を行う必要がある。

【０００３】

【発明が解決しようとする課題】この発明の目的は、一回発行された電子現金を発行時に決められた額になるまで、何回も分割して利用できる電子現金の分割利用方法を提供することにある。

【０００４】
【課題を解決するための手段】請求項１の発明によれば、電子現金の額面を階層的構造テーブルの最上位ノードとし、使用最小単位を階層的構造テーブルの最下位層のノードとし、あるノードの直下の子ノードの該当金額の合計が、そのノードの該当金額とする階層的構造テーブルを定め、使用金額をノードで指定し、あるノードが一度使われた後は、そのノードのすべての先祖ノード、およびすべての子孫ノードは利用しない、かつノードは１回以上使用しないというルールを適用することにより電子現金の分割使用を可能とする。
【０００５】請求項２の発明によれば、電子現金を利用する者（以下、利用者という）が有する装置（以下、利用者側装置という）と、利用者より電子現金を受信する機関（以下、小売店という）が有する装置（以下、小売店側装置という）により電子現金を分割使用する請求項１記載の方法において、上記利用者側装置は電子現金の額面と対応した値Γ。を生成し、上記階層構造における使用金額と対応したノードと対応した値$\Omega_{i_1,\ldots,i_1}$を生成し、上記値Γ。と上記値$\Omega_{i_1,\ldots,i_1}$（Ｌ＝１，…，ｔ）を用いて、上記使用金額に対応するノードに対する値の剰余べき乗根
【０００６】
【数３】

$$X_{j_1-j_t}=\left[(\Omega_{j_1\cdots j_{t-1}}^{2^{t-1}j_t}\,\Omega_{j_1\cdots j_{t-2}}^{2^{t-2}j_{t-1}}\cdots\Omega_{j_1}^{2j_2}\Gamma_0)^{1/2^t}\bmod N\right]_{-1}$$

【０００７】を求め、〔…〕$_{-1}$はヤコビ記号であって、（$x_{i_1\ldots i_t}$／Ｎ）＝－１であり、この$x_{i_1\ldots i_t}$および電子現金を上記小売店側装置へ送り、上記小売店側装置は上記受信した$x_{i_1\ldots i_t}$が（$x_{i_1\ldots i_t}$／Ｎ）＝－１を満たすかを検証し、利用者側装置と同様の処理によりΓ。と$\Omega_{i_1\ldots i_1}$を生成し、
【０００８】
【数４】

$$X_{j_1-j_t}^{2^t}=d\,\Omega_{j_1\cdots j_{t-1}}^{2^{t-1}j_t}\,\Omega_{j_1\cdots j_{t-2}}^{2^{t-2}j_{t-2}}\cdots\Omega_{j_1}^{2j_2}\Gamma_0\bmod N$$

【０００９】を満たすかを検証し、以上の検証が正しければ、上記電子現金による上記使用金額の支払いを認める。つまりあるノードが一度使われた後は、そのノードと連結するすべての先祖ノードおよび子孫ノードは利用しないことを満たしていると認める。
【００１０】請求項３の発明によれば、電子現金を利用するる者（以下、利用者という）が有する装置（以下、利用者側装置という）と、利用者より電子現金を受信する機関（以下、小売店という）が有する装置（以下、小売店側装置という）により電子現金を分割使用する請求項１または２記載の方法において、小売店側装置は値Ｅ（＝０または１）を利用者側装置へ送り、利用者側装置は電子現金の額面および使用金額ノードと対応した値$\Lambda_{i_1\ldots i_t}$を生成し、値$\Lambda_{i_1\ldots i_t}$と値Ｅとから次の剰余平方根演算を行い、

$$Y_{i_1\ldots i_t}=\{(\Lambda_{i_1\ldots i_t})^{Y^2}\bmod N\}_{(-1)^E}$$

このY$_{i_1\ldots i_t}$を小売店側装置へ送り、小売店側装置は受信したY$_{i_1\ldots i_t}$について

$$(Y_{i_1\ldots i_t}/N)=(-1)^E$$

$$(Y_{i_1\ldots i_t})^2=d'\,f\Lambda(C\|j_1\|\cdots\|j_t\|N)\bmod N$$

を共に満足するかを検証し、正しければ上記電子現金による上記使用金額の支払いを認める。つまりノードの直下の子ノードの該当金額の合計が、そのノードの該当金額となるという条件を満たしていることになる。
【００１１】つまり、この発明においては、電子現金の構造に対応した階層構成のテーブルを構成し、電子現金利用時には、このテーブルの構造に対応させる形で、一定の額面金額内の現金を何回かに分割して使用可能としている。また、上記利用形態における不正使用を検出するため、上述のように利用者と小売店との確認で剰余べき乗根を利用することは、例えばウィリアムズ数と呼ばれる合成数を法とする偶数べき乗根を利用することであり、ここでは、２つの異なるタイプの偶数べき乗根を用いて、法である合成数の素因数分解ができるという事実が重要な役割をする。つまり、利用者が不正使用をすれば、法の素因数分解を通じて、利用者の秘密情報である利用者のＩＤが露見するしかけになっている。
【００１２】
【発明の実施の形態】
（１）まず電子現金の発行および使用するためのシステム構成の例を図１に示す。電子現金を発行する機関（以下、銀行という）の装置（以下、銀行側装置という）１００と、電子現金を発行される者（以下、利用者という）の装置（以下、利用者側装置という）２００と、利用者より電子現金を受領する機関（以下、小売店という）の装置（以下、小売店側装置という）３００とが通信回線等を介して接続している。
【００１３】（２）次に電子現金の利用者のプライバシを保証するために用いる利用許可証の発行処理について説明する。まず、銀行で口座を新たに開設した利用者が、利用許可証を銀行より発行してもらう場合について説明する。利用者側装置は利用者の識別情報ＩＤｐ（利用者の口座番号など）を含んだ秘密情報（利用者情報）より乱数で攪乱したＫ組のブラインド情報を作成し、銀行側装置は、そのブラインド情報の中でＫ／２組の情報の開示を求め、開示された情報が正しく作成されていれば、残りの未開示のＫ／２組の情報に対しブラインド署名を作成し利用者側装置に送信し、利用者側装置は、銀行側装置から受信したブラインド署名から利用者情報に対する銀行の署名を計算して、この銀行署名を利用許可証とする。

【００１４】銀行側装置は、利用許可証に対応する情報として、ディジタル署名で用いるＲＳＡ暗号の秘密鍵（dA，nA）および公開鍵（eA，nA）の対を作成しておき公開鍵eA，nAを公開しておく。一方、利用者側装置は、ディジタル署名で用いるＲＳＡ暗号の秘密鍵（dP，nP）および公開鍵（eP，nP）の対を作成しておき、（eP，nP）をＩＤｐと対にして公開しておく。

【００１５】利用者が銀行から利用認可証を発行してもらう手順は、以下の通り。銀行側装置と利用者側装置の間の交信例を図２に示す。利用者側装置２００の利用許可証発行処理の構成を図３に、銀行側装置のそれを図４にそれぞれ示す。以下では、ｉ＝１，２，…，Ｋとする。

ステップ１　利用者側装置は、乱数発生器２０１を用いて乱数a_i，r_iを生成して、ＩＤｐと共に連結器２０４に入力し、その出力ＩＤｐ‖a_iを一方向ハッシュ関数演算器２０５に入力し、さらにその出力ｇ（ＩＤｐ‖a_i）を利用者の署名用秘密鍵（dP，nP）と共にＲＳＡ署名器２０６に入力し、$(g(IDp \| a_i))^{dP} \bmod nP$を求める。

【００１６】ステップ２　署名器２０６の出力を$ID_P \| a_i$と共に連結器２０７に入力して、$S_i = ID_P \| a_i \| (g(ID_P \| a_i))^{dP} \bmod nP$を求める。さらに、$S_i$を分割器２０８に入力し、$S_i = S_{1,i} \| S_{2,i}$になるような$S_{1,i}$と$S_{2,i}$を求める。

ステップ３　素数生成器２０２を用いて、$P_i \equiv 3 \pmod 8$および$Q_i \equiv 7 \pmod 8$を満足する２つの素数P_i，Q_iを生成して、乗算器２０３を用いてその積$N_i = P_i Q_i$を求める。

【００１７】ステップ４　$S_{1,i}$および$S_{2,i}$をN_iと共に剰余べき乗演算器２０９および２１１にそれぞれ入力し、$I_{1,i} = (S_{1,i})^2 \bmod N_i$と$I_{2,i} = (S_{2,i})^2 \bmod N_i$を求め、それらを連結器２１０に入力し$I_i = I_{1,i} \| I_{2,i}$を計算する。

ステップ５　N_i，I_iを連結器２１２に入力し、その出力$I_i \| N_i$を一方向ハッシュ関数演算器２１３に入力し、$g(I_i \| N_i)$を得る。一方、r_iを銀行の公開鍵（eA，nA）と共にＲＳＡ暗号器２１５に入力し、$(r_i)^{eA} \bmod nA$を求める。次に、それら出力を剰余乗算器２１４に入力し、ブラインド情報$W_i = (r_i)^{eA} g(I_i \| N_i) \bmod nA$を求めて、$W_i$（ｉ＝１，２，…，Ｋ）を銀行側装置に送信する。

【００１８】ステップ６　次に、銀行側装置は、利用者側装置に、そのうちのＫ／２組のa_i，P_i，Q_i（$g(IDp \| a_i))^{dP} \bmod np$，ＩＤｐ，$r_i$を開示させて、利用者側装置がステップ１からステップ５を正しく実行していることを確認する。このため、銀行側装置１００は、１からＫの中からランダムにＫ／２個を選び、それを開示要求として利用者側装置に送信する（ここでは、表記を簡単にするため、Ｋ／２＋１，Ｋ／２＋２，…，Ｋが開示指定されたと仮定して説明する）。Ｋ／２個でなく、Ｋの一部であればよいが、Ｋ／２とすると処理効率がよい。

【００１９】ステップ７　利用者側装置２００は、銀行側装置から開示要求を受信すると、銀行側装置の指示するＫ／２組のa_i，P_i，Q_i，$(g(IDp \| a_i))^{dP} \bmod np$，ＩＤｐ，$r_i$を開示する。銀行側装置は、ｉが開示対象の時、次の手順を行う。

ステップ８　利用者側装置２００より受信したa_i，ＩＤｐより$(g(IDp \| a_i))^{dP} \bmod nP$の署名の正当性を利用者側装置の公開鍵（eP，nP）を用いて連結器１０４でa_iとＩＤｐを連結し、それを一方向ハッシュ関数演算器１０５へ供給し、一方$(g(IDp \| a_i))^{dP} \bmod nP$とnP，ePとをＲＳＡ暗号器１０７に入力して暗号化しこの結果と演算器１０５の出力とを比較器１１１で検証する。ここで、検証に合格しなければ処理を中断する。

【００２０】ステップ９　利用者側装置２００より受信したa_i，P_i，Q_i，$(g(IDp \| a_i))^{dP} \bmod nP$ＩＤｐから、乗算器１０３を用いて$N_i = P_i Q_i$を求め、さらに、連結器１０８で$a_i$，ＩＤｐを連結して$S_i$とし、$S_i$を分割器１０９で分割し、それぞれ剰余べき乗演算器１１０，１１２でN_iと剰余べき演算し、その結果を連結器１１１で連結してI_iを求める。

【００２１】ステップ１０　上で計算したI_i，N_iを連結器１１３で連結し、更に一方向ハッシュ関数演算器１１４に供給し、受信したr_iと公開鍵eA，nAをＲＳＡ暗号器１１７へ供給し、その出力と演算器１１４の出力とを剰余乗算器１１５へ供給して$W'_i = (r_i)^{eA} g(I_i \| N_i) \bmod nA$を計算する。

ステップ１１　前に受信したW_iの値とW'_iの値を比較器１１６で比較し、一致すれば合格とし、不合格の場合、処理を中断する。銀行側装置は、Ｋ／２個のすべてのｉについて上記の検査を行い、いずれかの検査に不合格のときには、以降の処理を中止する。すべての検査に合格のときには、銀行側装置は、開示対象でないｉ＝１，…，Ｋ／２に対して、次の手順でブラインド署名を行う。

【００２２】ステップ１２　剰余乗算器１１８とＲＳＡ署名作成器１１９を用いて、銀行側装置の署名用秘密鍵（nA，dA）とW_iとから$W = (\Pi W_i)^{dA} \bmod nA$を求め、つまりブラインド署名を作り、このWを利用者側装置に送信する。

ステップ１３　利用者側装置は、銀行側装置からWを受信すると、r_iと公開鍵（eA，nA）から、剰余乗算器２１６、剰余除算器２１７を用いて利用許可証$B = W / (\Pi r_i) \bmod nA = (\Pi g(I_i \| N_i)^{dA} \bmod nA$を計算する。Πはｉ＝１からＫ／２までである。

【００２３】（３）更に利用許可証を用いて電子現金を発行してもらう処理を説明する。次に、利用者が銀行か

ら電子現金を発行してもらう手順を示す。まず、銀行側装置は、電子現金の金額に対応する情報として、ＲＳＡディジタル署名で用いる秘密鍵（dA′ nA′）および公開鍵（eA′ nA′）の対を作成しておき、（eA′ nA′）をその金額と共に公開しておく。ここで、銀行側装置と利用者側装置の間の交信例を図５に示す。利用者側装置２００および銀行側装置１００の各電子現金発行処理の構成を図６Ａ，Ｂにそれぞれ示す。以下では、ｉ＝１，２，…，Ｋ／２とする。

【００２４】ステップ１　乱数発生器２０１を用いて生成した乱数ｂ，ｒと利用許可証Ｂおよび電子現金の発行金額に相当する銀行側装置の公開鍵（eA′，nA′）からｒとeA′ nA′とをＲＳＡ暗号器２１５へ供給して認証用情報を生成し、これとｈ，Ｂとから連結器２０４、一方向ハッシュ関数演算器２０５、剰余乗算器２１４を用いて、

$Z = r^{eA'} g(B \| b) \bmod nA'$

を計算して引き出す電子現金の金額に相当するブラインド情報を得る。

【００２５】ステップ２　このＺを電子現金の金額情報と共に銀行側装置へ送る。

ステップ３　Ｚを受信した銀行側装置は、Ｚと電子現金の金額に対応する秘密鍵（dA′ nA′）とをＲＳＡ署名生成器１１９に入力し、$Z' = Z^{dA'} \bmod nA'$ を求め、つまり引出し金額に相当するブラインド署名を作成してそれを利用者側装置に送付する。同時に、利用者側装置の口座から該当する金額を引き落とすか、利用者側装置から該当する金額を受領する。

【００２６】ステップ４　銀行側装置よりＺ′を受信した利用者は、乱数ｒと銀行側装置より受信した情報Ｚ′およびnA′ 剰余除算器２１７に入力し、認証用情報および利用許可証に対する銀行側装置の署名

$C = Z' / r \bmod nA' = (g(B \| b))^{dA'} \bmod nA'$

を求める。ここで、Ｃが電子現金に相当する。

【００２７】（４）以上のようにして発行された電子現金をこの発明により分割使用する方法を説明する。利用者が、電子現金を用いて小売店で支払いをする場合について説明する。まず、電子現金の金額およびその使用最小単位（例えば、１０円単位等）に対応して、階層的構造テーブルが定められる。たとえば、２５円単位で、１００円の紙幣を利用する場合の階層的構造テーブルを図７Ａに示す。電子現金の額面１００円は階層的構造テーブルの最上位とされ、使用最小単位２５円は階層的構造テーブルの最下位層とされる。ここで、例えば、７５円を使う場合、ノード００とノード０１０が該当するノードとなる。この該当ノードは、以下のルールで定められる。

【００２８】１．あるノードの直下の子ノードの該当金額の合計が、そのノードの該当金額となる。

２．あるノードが一度使われた後は、そのノードと連結するすべての先祖ノードおよび子孫ノードは利用してはならない。

３．各ノードは、一回以上使用してはならない。

【００２９】このルールに従うと、先の例では、ノード００とノード０１０が使用された後で、使用できるノードは、ノード０１１（２５円）のみである。つまり、上のルールに従うことにより、使用できる合計金額は、額面通り１００円となると共に、２５円単位でどのような使い方でもできる。この階層的構造テーブルは、電子現金の額面金額を大きくし、さらに利用単位金額を小さくすれば、その階層が増えることになる。例えば、額面が１００万円で、１円単位で利用できる電子現金の場合、その階層は、およそ２０となる（$\log_2 1000000 \fallingdotseq 20$）。

【００３０】次に、利用者側装置と小売店側装置の間の交信例を図８に示す。小売店側装置３００と利用者側装置２００の電子現金利用手続の処理構成をそれぞれ図９，１０に示す。多くの場合、利用金額に相当する階層構造テーブルの該当ノードは複数あるが、各ノードに対応する処理は、基本的に同じアルゴリズムで行われ、それぞれのノードの処理を並列に行うことができるため、以下では、１つのノードに対する処理のみを説明する。この該当ノードをノード$j_1\ j_2 \cdots j_t$（$j_1 \in \{0, 1\}$）とする（図７Ｂ）。また、以下では、ｉ＝１，２，…，Ｋ／２とする。

【００３１】なお、以下の手順で用いる記号の意味をここでまとめて記しておく。

【００３２】

【数５】

9　　10

$$\left[x^{1/2^t} \bmod N\right]_1 = y'$$

では、$y'^{2^t} = x \bmod N$, $(y'/N)=1$, かつ $0<y'<N/2$. (1≦t)

$$\left[x^{1/2^t} \bmod N\right]_{-1} = y''$$

では、$y''^{2^t} = x \bmod N$, $(y''/N)=-1$, かつ $0<y''<N/2$. (1≦t)

$$\langle z\rangle_{QR} = dz \bmod N$$

では、d∈{±1, ±2} かつdzがNに関し平方剰余。

$$\langle z\rangle_1 = d'z \bmod N$$

では、d'∈{1, 2} かつ (d'z/N) = 1。

$$\langle z\rangle_{-1} = d''z \bmod N$$

では、d''∈{1, 2} かつ (d''z/N) = -1。

【００３３】なお、以上において、（／）は、ヤコビ記号を意味する。ヤコビ記号の効率的計算法は、例えば、藤崎、森田、山本著の「数論への出発（数学セミナー増刊）」（日本評論社）の１６６頁に記されている。

ステップ１　利用者側装置２００は、まず、C，N_i よりランダム関数Γ演算器２２０を用いて、$\Gamma_{i,0}$ を求める。

【００３４】

【数６】

$$\Gamma_{i,0} = \langle f_r(C \| 0 \| N_i)\rangle_{QR}$$

【００３５】次に、Cと利用金額と対応するノード$j_1 \cdots j_t$ とN_i をランダム関数Ω演算器２２１に入力し、$\Omega_{i,11\cdots11}$ （L＝１，…，ｔ）を生成する。

【００３６】

【数７】

$$\Omega_{i,j_1\cdots j_l} = \langle f_\alpha(C \| j_1 \| \cdots \| j_l \| N_i)\rangle_1$$

【００３７】さらに、$\Gamma_{i,0}$，$\Omega_{i,11\cdots11}$ （L＝１，…，ｔ），N_i より剰余べき乗演算器２２２、剰余乗算器２２３、剰余べき乗根演算器２２４を用いて、利用金額に対応するノードに対する値の剰余べき乗根$X_{i,11\cdots1t}$ を求める。ここでN_i はウィリアムズ数である。

【００３８】

【数８】

$$X_{i,j_1\cdots j_t} = \left[(\Omega_{i,j_1\cdots j_{t-1}}^{2^{t-1}j_t}\ \Omega_{i,j_1\cdots j_{t-2}}^{2^{t-2}j_{t-1}} \cdots \Omega_{i,j_1}^{2j_2}\ \Gamma_{i,0})^{1/2^t} \bmod N_i\right]_{-1}$$

【００３９】ステップ２　利用者側装置２００は、b，（I_i，N_i，$X_{i,11\cdots1t}$）（i＝１，…，K／２）および（B，C）を小売店側装置３００に送る。

ステップ３　小売店側装置３００は、連結器３０４、一方向ハッシュ関数演算器３０５、剰余乗算器３０９、RSA暗号器３１０、比較器３１１を用いて、公開鍵（eA，nA）によりBの$I_i \| N_i$ に対する署名の正当性を（つまり、$B^{eA} = (\Pi g(I_i \| N_i)) \bmod nA$が成立するかどうかを、Πはi＝１からK／２まで）、また、連結器３１２、一方向ハッシュ関数演算器３１３、RSA暗号器３１４、比較器３１５を用いて公開鍵（eA′，nA′）によりCのB‖bに対する署名の正当性を（つまり、$C^{eA'} = (g(B \| b)) \bmod nA'$ が成立するかどうかを）検査する。この検査が、不合格のときは以降の処理を中止する。

【００４０】ステップ４　小売店側装置３００は、ヤコビ記号演算器３１６および比較器３１７を用いて、$X_{i,11\cdots1t}$ が以下の関係を満足するかどうかを検証する。この検査が、不合格のときは以降の処理を中止する。

$(X_{i,11\cdots1t}/N_i) = -1$，

次に、C，N_i よりランダム関数Γ演算器３２４を用いて、

【００４１】

【数９】

$$f_r(C \| 0 \| N_i)$$

【００４２】を求める。また、C，$j_1 \cdots j_t$，N_i をランダム関数Ω演算器３２１に入力し、$\Omega_{i,11\cdots11}$ （L＝１，…，ｔ）を生成する。

【００４３】

【数１０】

$$\Omega_{i,j_1\cdots j_l} = \langle f_\alpha(C \| j_1 \| \cdots \| j_l \| N_i)\rangle_1$$

【００４４】さらに、

【００４５】

【数１１】

$$f_r(C \| 0 \| N_i),\ \Omega_{i,j_1\cdots j_l}\ (l=1,\cdots,t),\ N_i$$

【００４６】より剰余べき乗演算器３２２、剰余乗算器

11

３２３、剰余除算器３１９、比較器３２０を用いて、$X_{1,i_1\cdots i_t}$ が以下の関係を満足するかどうかを検証する。この検査が、不合格のときは以降の処理を中止する。つまり、あるノードが一度使われた後は、そのノードと連結するすべての先祖ノードおよび子孫ノードは利用してはならないというルール２を満たしているかが検証される。

【００４７】

【数１２】

$$X_{i,j_1\cdots j_t}^{2^t} = d_i \Omega_{i,j_1\cdots j_{t-1}}^{2^{t-1}j_t} \Omega_{i,j_1\cdots j_{t-2}}^{2^{t-2}j_{t-1}} \cdots \Omega_{i,j_1}^{2j_2} \Gamma_{i,0} \bmod N_i$$

【００４８】ここで、d_i は、±１，±２のいずれかの値である。

ステップ５　小売店側装置は、乱数発生器３０１より取り出した値 $E_i \in \{0, 1\}$ （$i = 1, \cdots, K/2$）を利用者側装置に質問情報として送付する。

ステップ６　利用者側装置は、ランダム関数Λ演算器２２５を用いて、C，$j_1 \ldots j_t$，N_i より $\Lambda_{i,i_1\cdots i_t}$ を計算する。

【００４９】

【数１３】

$$\Lambda_{i,j_1\cdots j_t} = \left\langle f_A\left(C \| j_1 \| \cdots \| j_t \| N_i\right)\right\rangle_{QR}$$

【００５０】次に、剰余平方根演算器２２６を用いて、$\Lambda_{i,i_1\cdots i_t}$ および E_i より、$Y_{i,i_1\cdots i_t}$ を計算する。

【００５１】

【数１４】

$$Y_{i,j_1\cdots j_t} = \left[(\Lambda_{i,j_1\cdots j_t})^{1/2} \bmod N_i\right]_{(-1)^{E_i}}$$

【００５２】利用者側装置は、$Y_{i,i_1\cdots i_t}$ を小売店側装置に送る。

ステップ７　小売店は、ヤコビ記号演算器３２５および比較器３２６を用いて、$Y_{i,i_1\cdots i_t}$ が以下の関係を満足するかどうかを検証する。この検査が、不合格のときは以降の処理を中止する。

$(Y_{i,i_1\cdots i_t} / N_i) = (-1)^{E_i}$

次に、C，$j_1 \cdots j_t$，N_i をランダム関数Λ演算器３２８に入力し、さらにその出力および $Y_{i,i_1\cdots i_t}$，N_i に対し、剰余べき乗演算器３２７、剰余除算器３２９、比較器３３０を用いて、以下の関係を満足するかどうかを検証する。

【００５３】

【数１５】

$$(Y_{i,j_1\cdots j_t})^2 = d'_i f_A\left(C \| j_1 \| \cdots \| j_t \| N_i\right) \bmod N_i$$

【００５４】ここで、d'_i は、±１，±２のいずれかの値である。この検査に合格すれば、小売店側装置は、

12

その電子現金のノード $j_1 \cdots j_t$ に該当する金額の支払を正当なものとみなし、それを受け取る。つまり、これらの検証によりあるノードの直下の子ノードの該当金額の合計が、そのノードの該当金額となるというルール１の条件を満たしているかの検証を行っている。

【００５５】（５）決済

最後に、小売店と銀行の間の決済方法について説明する。小売店側装置３００は、利用者側装置２００との電子現金利用時の交信履歴Ｈを銀行側装置に提出し、銀行側装置から該当する金額の支払いを受ける。銀行側装置は、Ｈの正当性を検査し、検査に合格すれば、Ｈを記憶して、小売店の口座へ該当する金額を払い込む。銀行側装置は、電子現金の不正利用を見つけると、Ｈを取り出して、それらの情報より不正者のＩＤを確定する。

【００５６】つまり第２１段落に記載されたルール２．に違反した場合、子ノードに対応するＸを２乗してゆき、親ノードの平方根でヤコビ記号が１となるものを得ることと、親ノードに対応するＸは、親ノードの平方根でヤコビ記号が－１となるものであることから、ヤコビ記号が１となる平方根と－１となる平方根が揃ったことにより、Ｎを素因数分解することができ、Ｎの素因数を用いて、Ｉから利用者の秘密情報Ｓを計算でき、またルール３．に違反した場合、Ｅはランダムに１か－１かが指定されたものであり、ＹはΛの平方根でヤコビ記号がＥにより指定されたものだから、同じΛを用いてＹを生成すると、１／２の確率でヤコビ記号が１と－１となる平方根が揃うことになり、Ｋ／２個の添字ｉについて手続きを実行すれば、ヤコビ記号が１となる平方根と－１となる平方根が圧倒的確率で揃うことにより、Ｎを素因数分解することができ、Ｎの素因数を用いて、Ｉから利用者の秘密情報Ｓを計算できる。

【００５７】上述において、利用許可証Ｂ，電子現金Ｃに対する検証は他の手法を用いてもよく、従って上述においてｉ＝０としてもよい。

【００５８】

【発明の効果】この発明は、階層的構造テーブルを用い、そのノードにより使用金額を決定することにより、一回発行された電子現金を発行時に決められた額になるまで、何回も分割して利用できる。

【図面の簡単な説明】

【図１】この発明が適用されるシステム例を示すブロック図。

【図２】利用許可証発行手続における交信例を示す図。

【図３】利用者側装置における利用許可証発行処理の構成を示すブロック図。

【図４】銀行側装置における利用許可証発行処理の構成を示すブロック図。

【図５】電子現金発行手順における交信例を示す図。

【図６】Ａ，Ｂはそれぞれ電子現金発行処理における利用者側装置および銀行側装置の各構成を示すブロック

図。

【図７】電子現金の階層的構造テーブルを示す図。

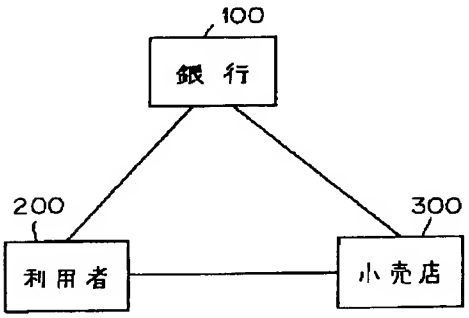
【図８】この発明による電子現金の利用手続における交信例を示す図。

＊【図９】図８の交信における利用者側装置での電子現金利用処理の構成を示すブロック図。

【図１０】図８の交信における小売店側装置での電子現金利用処理の構成を示すブロック図。

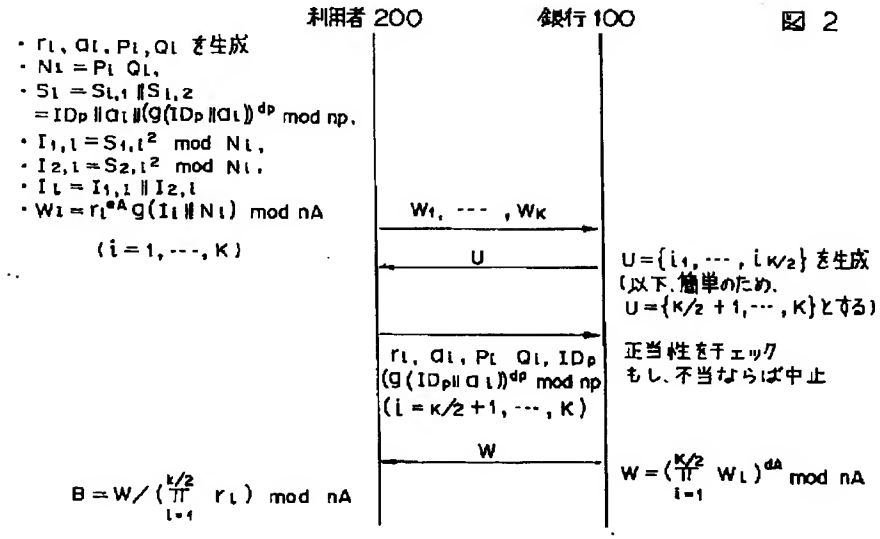
【図１】

図 1



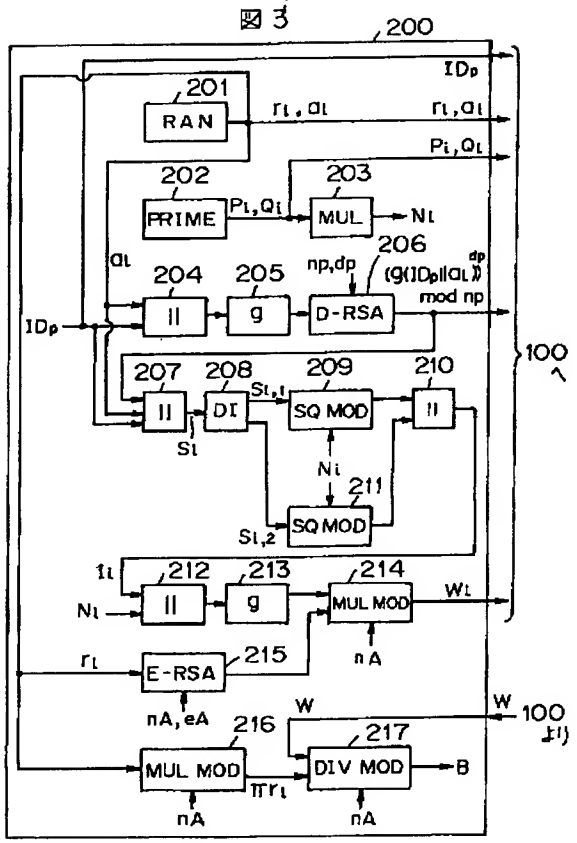
【図２】

図 2

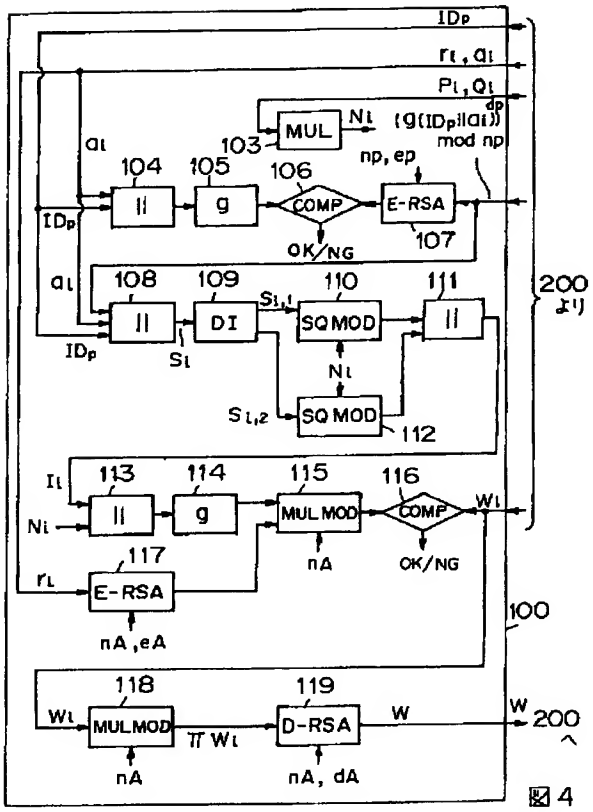


【図3】

図3

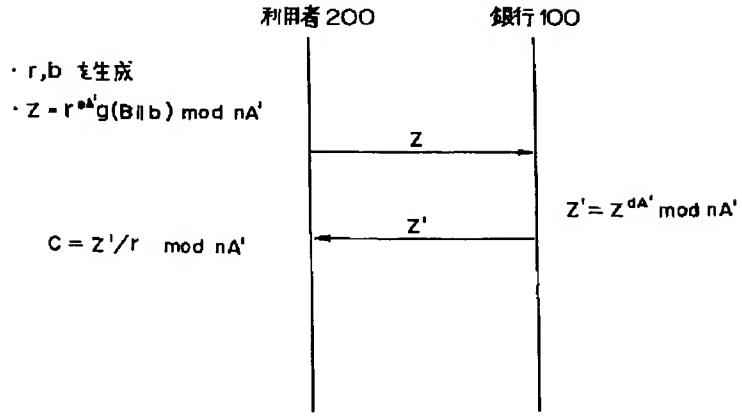

200
ID_p
201
RAN
r_t, a_t
P_t, Q_t
202
PRIME
203
MUL
N_t
a_t
204
205
206
g
D-RSA
np, dp
mod np
207
208
209
210
DI
SQ MOD
S_t,1
S_t
N_t
211
S_t,2
I_t
212
213
214
MUL MOD
W_t
r_t
215
E-RSA
nA, eA
nA
W
216
217
MUL MOD
DIV MOD
B
100へ
100より

【図4】


ID_p
r_t, a_t
P_t, Q_t
MUL
N_t
103
104
105
106
COMP
E-RSA
107
OK/NG
108
109
110
111
DI
SQ MOD
112
113
114
115
116
MUL MOD
117
118
119
D-RSA
200より
100
200へ
nA, dA
図4

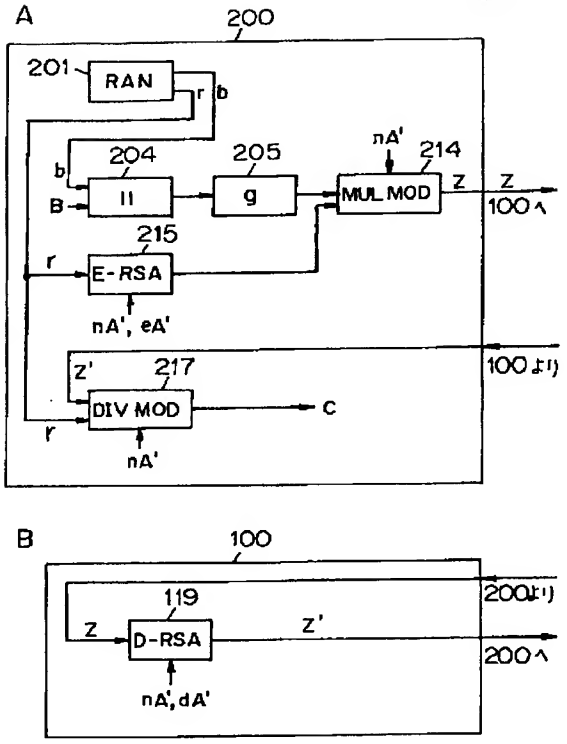
【図5】

図5


利用者200
銀行100
・r,b を生成
・Z = r^eA' g(B||b) mod nA'
Z
Z'
Z' = Z^dA' mod nA'
C = Z'/r mod nA'

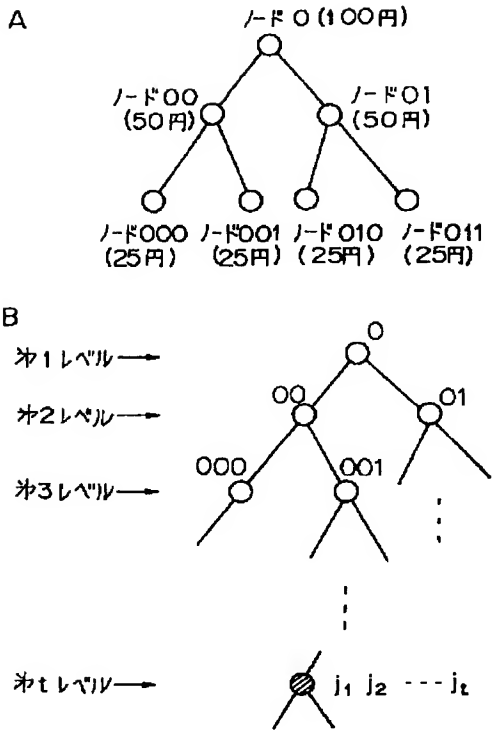
【図６】

図 6



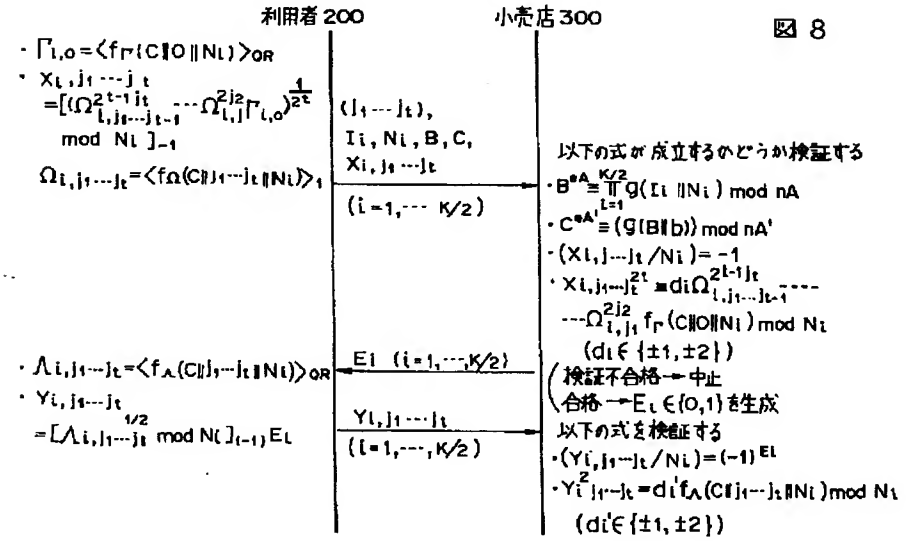
【図７】

図 7



【図８】

図 8



【図９】

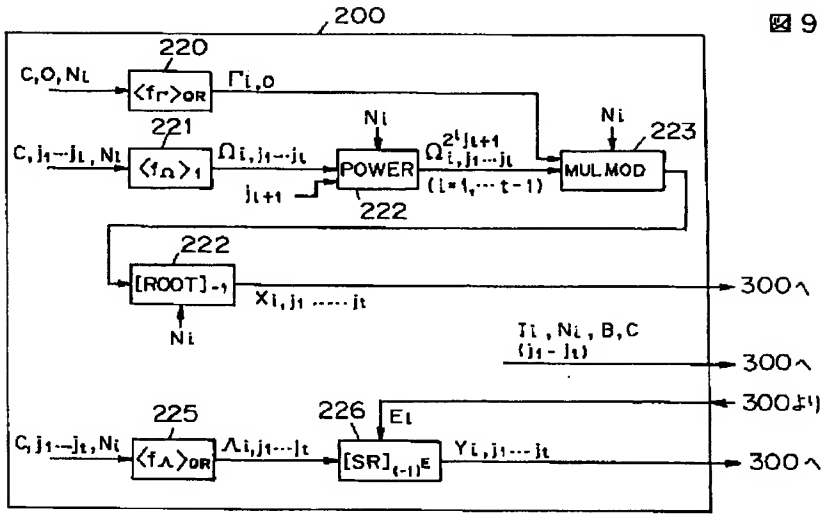

200
220
C,O,Nt
<fr>OR
Γi,o
221
C,j1--jt,Nt
<fΩ>1
Ωi,j1--jt
POWER
Nt
Ni
223
MULMOD
jt+1
222
[ROOT]-1
Xi,j1 ..... jt
300へ
Ni
It,Ni,B,C
(j1 - jt)
300へ
300より
225
226
Et
C,j1--jt,Ni
<fΛ>OR
Λi,j1---jt
[SR](t-1)E
Yi,j1---jt
300へ

図９

【図１０】

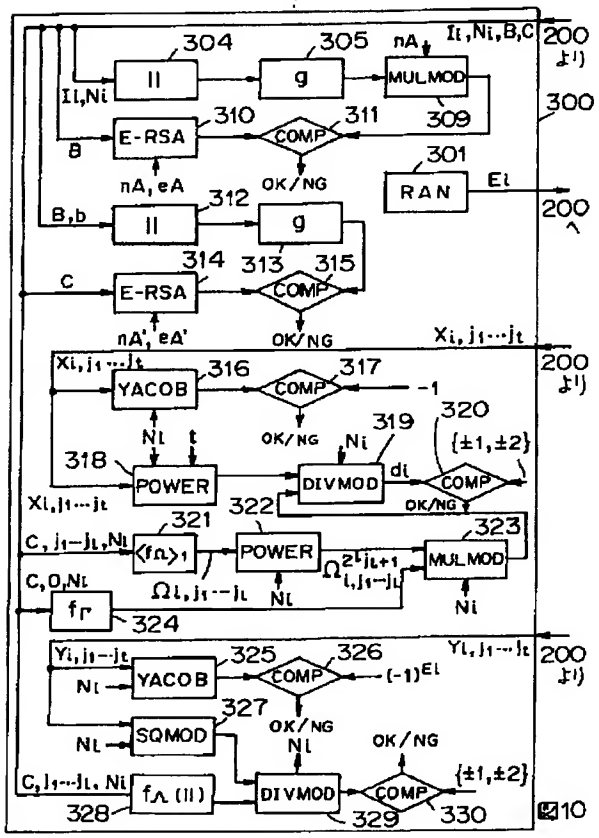

304
305
nA
It,Ni,B,C
200より
II
g
MULMOD
It,Ni
300
E-RSA
310
COMP
311
309
B
301
RAN
Et
200へ
nA,eA
OK/NG
312
B,b
II
g
314
313
315
C
E-RSA
COMP
nA',eA'
OK/NG
Xi,j1---jt
Xi,j1---jt
YACOB
316
COMP
317
-1
200より
Nt
t
OK/NG
Ni
319
320
{±1,±2}
318
POWER
DIVMOD
di
COMP
Xi,j1---jt
322
OK/NG
C,j1--jt,Nt
321
<fΩ>1
POWER
323
MULMOD
C,O,Nt
Ωi,j1--jt
Nt
Ni
fr
324
Yi,j1--jt
Yi,j1---jt
200より
325
326
YACOB
COMP
(-1)Et
Nt
327
OK/NG
SQMOD
Nt
Nt
OK/NG
C,j1---jt,Ni
fΛ(II)
DIVMOD
COMP
{±1,±2}
328
329
330

図10

フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
			Ｇ０７Ｆ　7/08		Ｂ